BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12)(19)(CA) **Demande-Application**

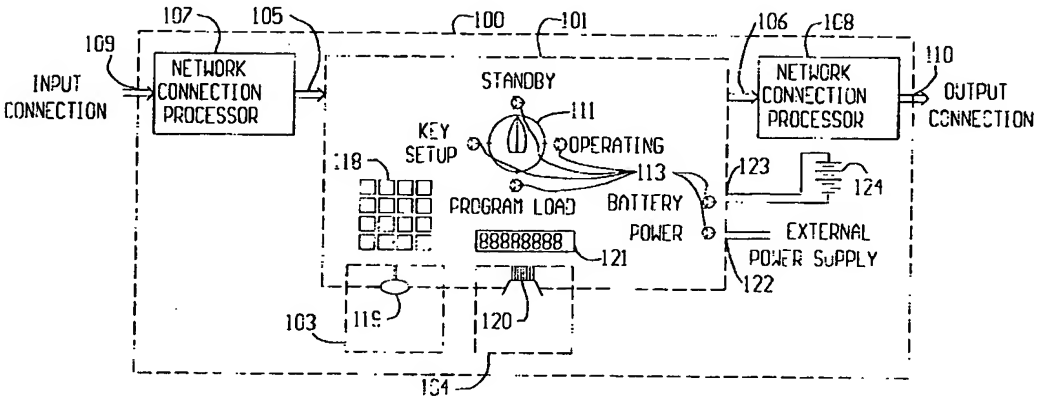
(21)(A1) **2,271,178**
(22) 1999/05/06
(43) 1999/07/06

(72) MOREAU, Thierry, CA
(71) CONNOTECH EXPERTS-CONSEILS INC., CA

(51) Int.Cl.[6] H04L 9/30

(54) **APPAREIL CRYPTOGRAPHIQUE A CLE REVELEE COTE-SERVEUR AVEC CLES SECRETES DE PROTECTION ET D'ISOLEMENT DE RESEAUX PUBLICS**

(54) **SERVER-SIDE PUBLIC KEY CRYPTOGRAPHY APPARATUS WITH PRIVATE KEY PROTECTION AND ISOLATION FROM PUBLIC NETWORKS**



(57) A server-server public-key cryptography apparatus is disclosed for use in the computer facilities of central organizations, e.g. on-line service providers. The apparatus has two network connections of the type common to computer networks, used respectively for exclusively receiving input data and exclusively transmitting output data for some elementary private key computation (digital signature, public key decryption, secret key establishment primitive based on a public key algorithm). The secrecy of this private key is supported by a number of the present invention features. Among others, are provided the cryptographic key management operations needed to initially configure, operate, maintain, and re-install in the case of disaster recovery. In operations, the access to the elementary private key computation has to be restricted to those computer applications that are the legitimate users of the private key. The one-way input connection, the one-way output connection, and some features of the cryptographic key management operations are provided to secure this restricted access to the function performed by the secure computing device.

ABSTRACT

A server-server public-key cryptography apparatus is disclosed for use in the computer facilities of central organizations, e.g. on-line service providers. The apparatus has two network connections of the type common to computer networks, used respectively for exclusively receiving input data and exclusively transmitting output data for some elementary private key computation (digital signature, public key decryption, secret key establishment primitive based on a public key algorithm). The secrecy of this private key is supported by a number of the present invention features. Among others, are provided the cryptographic key management operations needed to initially configure, operate, maintain, and re-install in the case of disaster recovery. In operations, the access to the elementary private key computation has to be restricted to those computer applications that are the legitimate users of the private key. The one-way input connection, the one-way output connection, and some features of the cryptographic key management operations are provided to secure this restricted access to the function performed by the secure computing device.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1 A secure cryptographic device implementing a public key cryptography primitive with a one-way input connection and a one-way output connection.

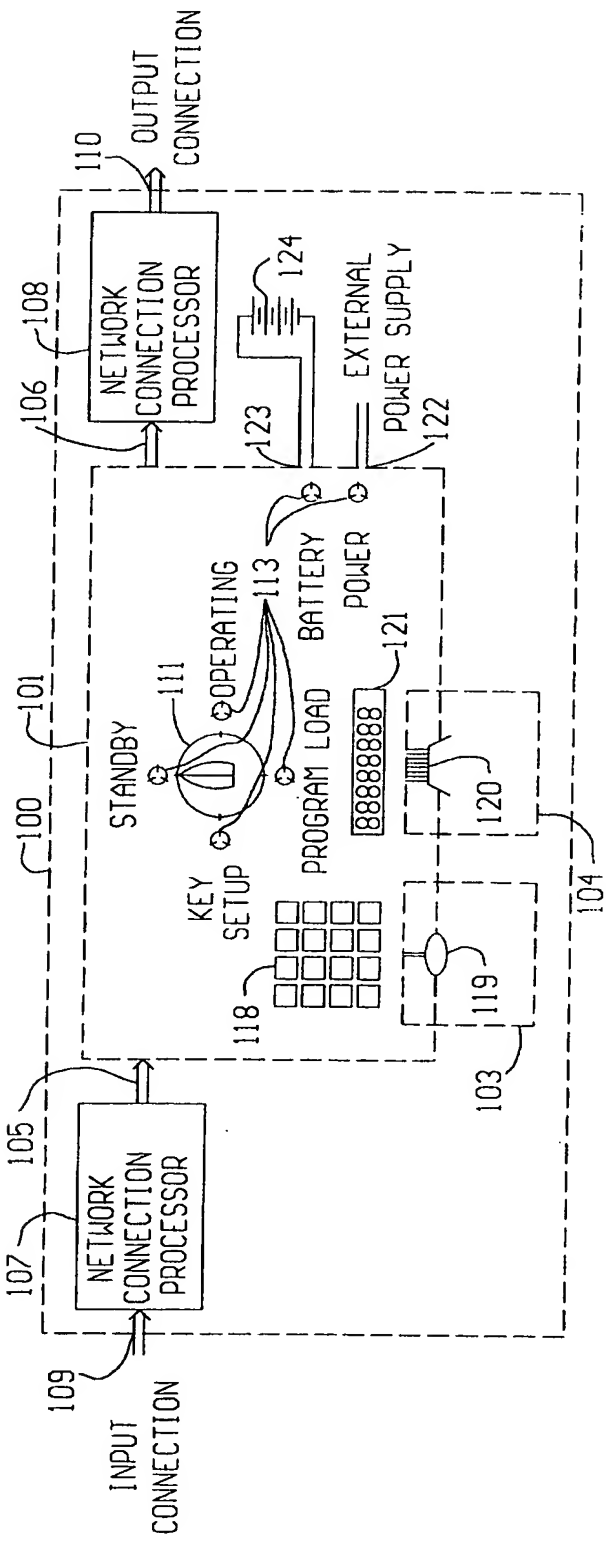

OUTPUT CONNECTION
110
NETWORK CONNECTION PROCESSOR
108
106
124
EXTERNAL POWER SUPPLY
123
122
BATTERY POWER
OPERATING
113
111
STANDBY
101
121
88888888
PROGRAM LOAD
120
100
KEY SETUP
104
118
119
103
105
NETWORK CONNECTION PROCESSOR
107
109
INPUT CONNECTION

Figure 1

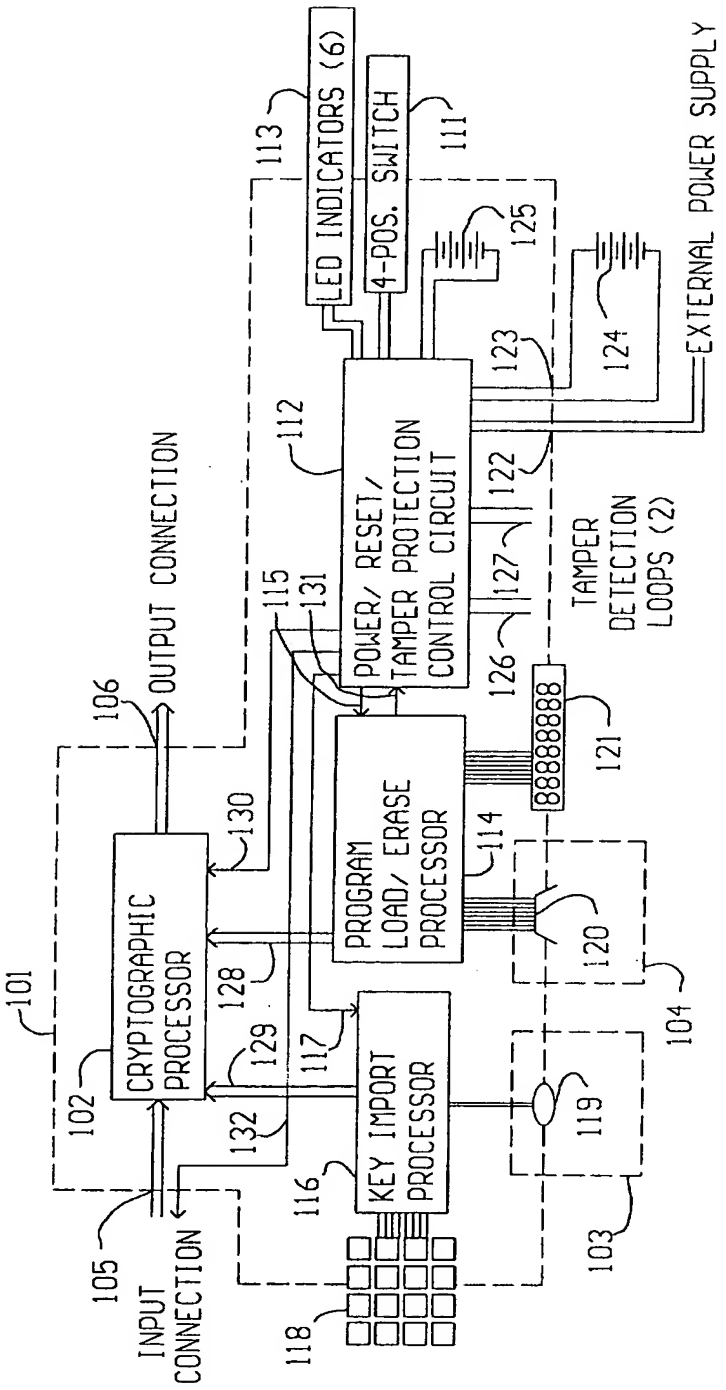

101
102
CRYPTOGRAPHIC PROCESSOR
103
104
105
INPUT CONNECTION
106
OUTPUT CONNECTION
112
POWER/ RESET/ TAMPER PROTECTION CONTROL CIRCUIT
113
LED INDICATORS (6)
111
4-POS. SWITCH
114
PROGRAM LOAD/ ERASE PROCESSOR
116
KEY IMPORT PROCESSOR
117
118
119
120
121
88888888
122
123
124
125
126
127
128
129
130
131
132
TAMPER DETECTION LOOPS (2)
EXTERNAL POWER SUPPLY

Figure 2

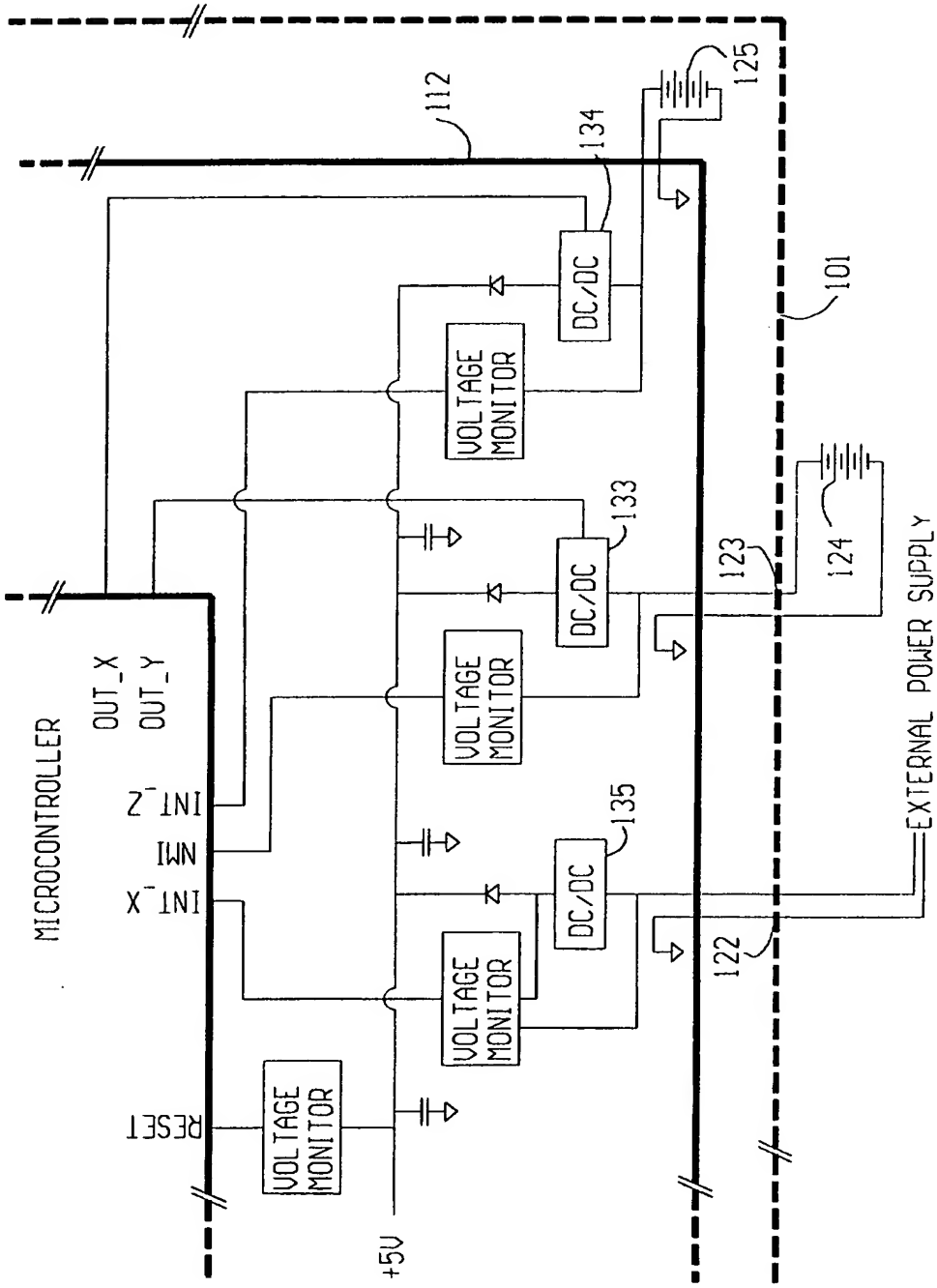

MICROCONTROLLER
OUT_X
OUT_Y
INT_Z
NMI
INT_X
RESET
+5V
VOLTAGE MONITOR
VOLTAGE MONITOR
VOLTAGE MONITOR
VOLTAGE MONITOR
DC/DC
DC/DC
DC/DC
112
134
133
135
101
125
123
124
122
EXTERNAL POWER SUPPLY

Figure 3

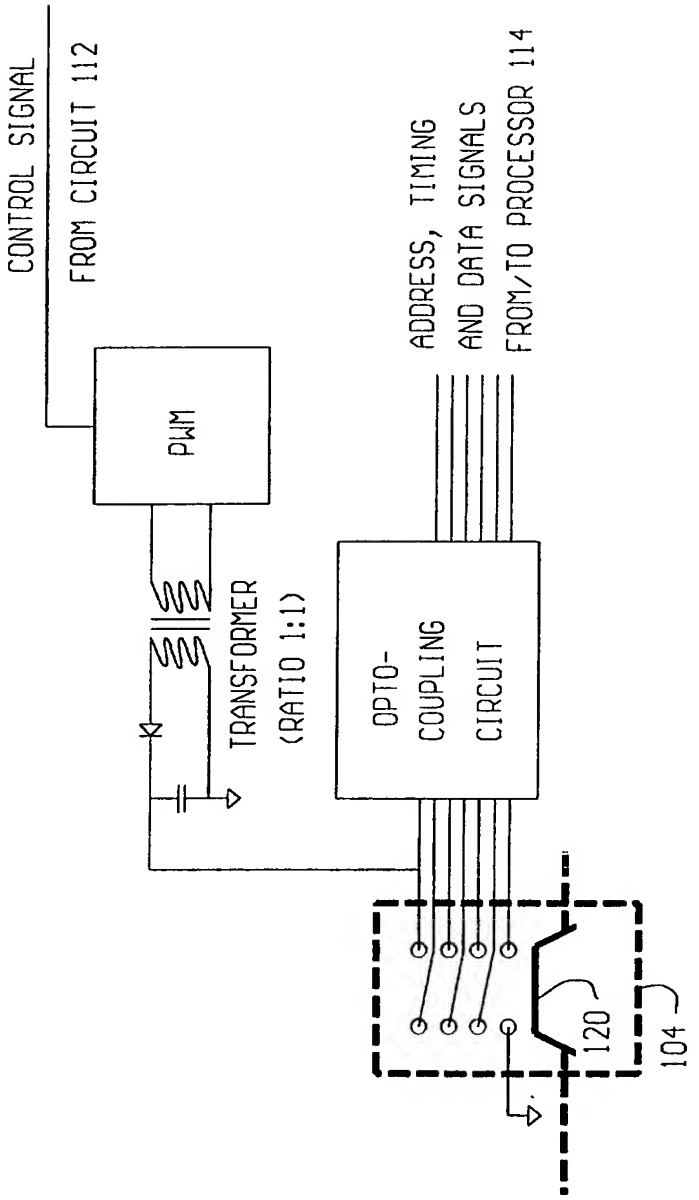

CONTROL SIGNAL
FROM CIRCUIT 112
PWM
TRANSFORMER
(RATIO 1:1)
OPTO-
COUPLING
CIRCUIT
ADDRESS, TIMING
AND DATA SIGNALS
FROM/TO PROCESSOR 114
120
104

Figure 4

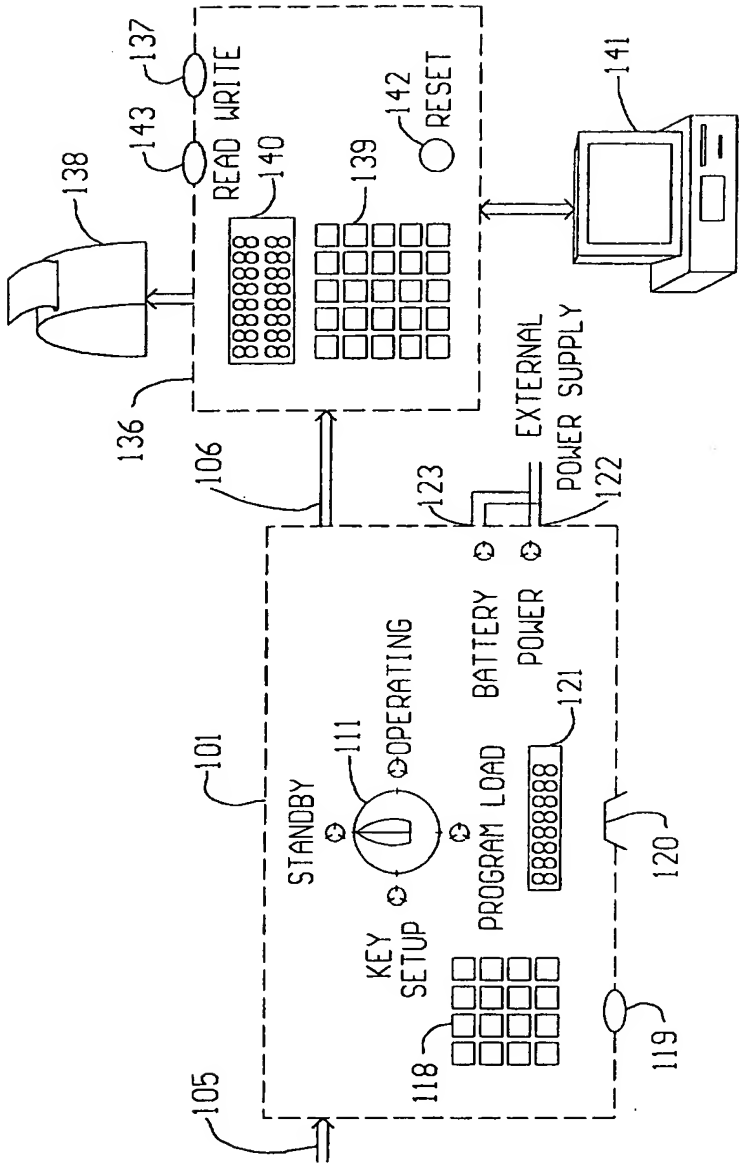

138
137
143
READ WRITE
140
139
142
RESET
141
88888888
88888888
136
106
123
EXTERNAL
POWER SUPPLY
122
101
111
STANDBY
OPERATING
BATTERY
POWER
121
PROGRAM LOAD
88888888
KEY
SETUP
120
118
119
105

Figure 5